

The following words are very common and were not included in your search: a for. [\[details\]](#)

Web Results 1 - 10 of about 495 for tygar yee a system for using physically secure coprocessors. (0.42 se

Dyad: A System for Using Physically Secure Coprocessors - Tygar ...
 ... html More @inproceedings{ tygar94dyad, author = "JD Tygar and Bennet Yee", title =
 "Dyad: {A} System for Using Physically Secure Coprocessors", booktitle = "{IP ...
 citeseer.ist.psu.edu/tygar91dyad.html - 28k - [Cached](#) - [Similar pages](#)

Citations: Dyad: A system for using physically secure coprocessors ...
 JD Tygar and Bennet Yee. Dyad: A system for using physically secure coprocessors.
 Technical report, Carnegie Mellon University, May 1991. CMU-CS-91-140R. ...
 citeseer.ist.psu.edu/context/146640/7518 - 28k - [Cached](#) - [Similar pages](#)
[\[More results from citeseer.ist.psu.edu \]](#)

IP Workshop - Tygar/Yee: Dyad

Dyad: A System for Using Physically Secure Coprocessors. by JD Tygar and Bennet
 Yee. ABSTRACT. Physically secure coprocessors, as used ...
[www.cni.org/docs/ima/ip-workshop/Tygar.Yee.html](#) - 101k - Feb 2, 2005 - [Cached](#) - [Similar pages](#)

Dyad: A System for Using Physically Secure Coprocessors

著者 JD Tygar, Bennet Yee タイトル Dyad: A System for Using Physically Secure
 Coprocessors 日時 May 1991 概要 The Dyad project at Carnegie Mellon ...
[plitecan.com/bib/Tygar_CMUCS91140R.html](#) - 4k - [Cached](#) - [Similar pages](#)

[PDF] Using a High-Performance, Programmable Secure Coprocessor

File Format: PDF/Adobe Acrobat - [View as HTML](#)
 ... Using secure coprocessors to build practical e-commerce applications requires ... Yee's
 work 16, 22, 23 explores these ... from even the operating system. Thus, an ...
[www.cs.dartmouth.edu/~sws/papers/fc98.pdf](#) - [Similar pages](#)

[PDF] Magic Boxes and Boots: Security in Hardware

File Format: PDF/Adobe Acrobat - [View as HTML](#)
 ... security, Apr. 1999, pp. 831-860. • JD Tygar and BS Yee, Dyad: A System
 for Using Physically Secure Coprocessors, tech. report CMU ...
[www.cs.dartmouth.edu/~sws/papers/magic_boxes.pdf](#) - [Similar pages](#)
[\[More results from www.cs.dartmouth.edu \]](#)

Computer Magazine - Magic Boxes and Boots: Security in Hardware ...

... 1999, pp. 831-860. JD Tygar and BS Yee, Dyad: A System for Using Physically
 Secure Coprocessors, tech. report CMU-CS-91-140R, School ...
[www.computer.org/computer/ homepage/1004/security/sidebar.htm](#) - 17k - [Cached](#) - [Similar pages](#)

Bennet's Research Summary

... Information-Based Indicia system (earlier work with Tygar and Heintze ... The Triton
 system is joint work with Noriya Kobayashi (NEC). ... Copyright 2004 Bennet Yee. ...
[www.bennetyee.org/ucsd-pages/research_summary.html](#) - 14k - [Cached](#) - [Similar pages](#)

[PDF] Secure Coprocessors in Electronic Commerce Applications

File Format: PDF/Adobe Acrobat - [View as HTML](#)
 ... Bennet Yee JD Tygar Microsoft Corporation Carnegie Mellon University ... PA 15213

bsy@microsoft.com tygar@cs.cmu ... copying) in a capability-based protection system [...
www.cs.berkeley.edu/~tygar/ papers/Secure_coprocessors_in_e-comm.pdf - Similar pages

[PDF] Bennet Yee C Research areas Education

File Format: PDF/Adobe Acrobat - View as HTML

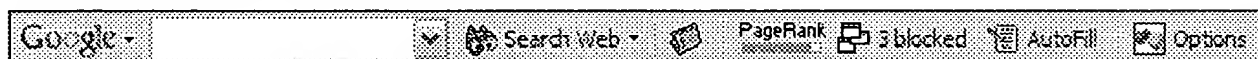
... Worked with Professors D. Tygar, R. Rashid, and A. Spector on the Strongbox, CAMELOT,
Mach ... Bennet Yee 5 ... Dyad: a system for using physically secure coprocessors. ...

www.cs.ucsd.edu/~bsy/cv.pdf - Similar pages

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

Free! Get the Google Toolbar. [Download Now](#) - [About Toolbar](#)



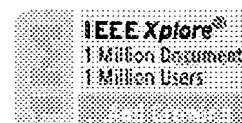
tygar yee a system for using physica Search

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied?](#) [Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE


[Membership](#) | [Publications/Services](#) | [Standards](#) | [Conferences](#) | [Careers/Jobs](#)

[Help](#) | [FAQ](#) | [Terms](#) | [IEEE Peer Review](#)
[Quick Links](#)

>> See

Welcome to IEEE Xplore

- ☐ Home
- ☐ What Can I Access?
- ☐ Log-out

Tables of Contents

- ☐ Journals & Magazines
- ☒ Conference Proceedings
- ☐ Standards

Search

- ☐ By Author
- ☐ Basic
- ☐ Advanced
- ☐ CrossRef

Member Services

- ☐ Join IEEE
- ☐ Establish IEEE Web Account
- ☐ Access the IEEE Member Digital Library

IEEE Enterprise

- ☐ Access the IEEE Enterprise File Cabinet

Print Format

Your search matched **2** of **1123491** documents.A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.**Refine This Search:**

You may refine your search by editing the current search expression or entering new one in the text box.

secure bootstrap

Search

☐ Check to search within this result set**Results Key:****JNL** = Journal or Magazine **CNF** = Conference **STD** = Standard**1 A secure active network environment architecture: realization in SwitchWare**

Alexander, D.S.; Arbaugh, W.A.; Keromytis, A.D.; Smith, J.M.;
 Network, IEEE, Volume: 12, Issue: 3, May-June 1998
 Pages:37 - 45

[\[Abstract\]](#) [\[PDF Full-Text \(2044 KB\)\]](#) **IEEE JNL**
2 Secure registration protocol for media appliances in wireless home networks

Taesombut, N.; Kumar, V.; Dubey, R.; Rangan, P.V.;
 Multimedia and Expo, 2003. ICME '03. Proceedings. 2003 International Confer-
 on, Volume: 3, 6-9 July 2003
 Pages:III - 109-12 vol.3

[\[Abstract\]](#) [\[PDF Full-Text \(343 KB\)\]](#) **IEEE CNF**

[Home](#) | [Log-out](#) | [Journals](#) | [Conference Proceedings](#) | [Standards](#) | [Search by Author](#) | [Basic Search](#) | [Advanced Search](#) | [Join IEEE](#) | [Web Account](#) |
[New this week](#) | [OPAC Linking Information](#) | [Your Feedback](#) | [Technical Support](#) | [Email Alerting](#) | [No Robots Please](#) | [Release Notes](#) | [IEEE Online Publications](#) | [Help](#) | [FAQ](#) | [Terms](#) | [Back to Top](#)

Copyright © 2004 IEEE — All rights reserved


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☐ The ACM Digital Library ☒ The Guide



THE GUIDE TO COMPUTING LITERATURE


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

 Terms used **operating system encryption**

Found 126,672 of 846,556

 Sort results by

[Save results to a Binder](#)
[Try an Advanced Search](#)

 Display results

[Search Tips](#)
[Try this search in The Digital Library](#)
☐ Open results in a new window

Results 1 - 20 of 200

 Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

 Relevance scale ☐ ☐ ☐ ☐ ☐

1 [Virtual machine monitors: Implementing an untrusted operating system on trusted hardware](#)

David Lie, Chandramohan A. Thekkath, Mark Horowitz

 October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

 Full text available: [pdf\(260.87 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Recently, there has been considerable interest in providing "trusted computing platforms" using hardware~----~TCPA and Palladium being the most publicly visible examples. In this paper we discuss our experience with building such a platform using a traditional time-sharing operating system executing on XOM~----~a processor architecture that provides copy protection and tamper-resistance functions. In XOM, only the processor is trusted; main memory and the operating system are not trusted. Our opera ...

Keywords: XOM, XOMOS, untrusted operating systems

2 [A database encryption system with subkeys](#)

George I. Davida, David L. Wells, John B. Kam

 June 1981 **ACM Transactions on Database Systems (TODS)**, Volume 6 Issue 2

 Full text available: [pdf\(1.16 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

A new cryptosystem that is suitable for database encryption is presented. The system has the important property of having subkeys that allow the encryption and decryption of fields within a record. The system is based on the Chinese Remainder Theorem.

Keywords: data security, databases, decryption, encryption, subkeys

3 [Low power scalable encryption for wireless systems](#)

James Goodman, Anantha P. Chandrakasan

 January 1998 **Wireless Networks**, Volume 4 Issue 1

 Full text available: [pdf\(7.39 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


Secure transmission of multimedia information (e.g., voice, video, data, etc.) is critical in many wireless network applications. Wireless transmission imposes constraints not found in typical wired systems such as low power consumption, tolerance to high bit error rates, and

scalability. A variety of low power techniques have been developed to reduce the power of several encryption algorithms. One key idea involves exploiting the variation in computation requirements to dynamically vary th ...

4 [Authentication in the Taos operating system](#)

Edward Wobber, Martín Abadi, Michael Burrows, Butler Lampson

February 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 1

Full text available:  [pdf\(1.85 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

We describe a design for security in a distributed system and its implementation. In our design, applications gain access to security services through a narrow interface. This interface provides a notion of identity that includes simple principals, groups, roles, and delegations. A new operating system component manages principals, credentials, and secure channels. It checks credentials according to the formal rules of a logic of authentication. Our implementation is efficient enough to sup ...

Keywords: cryptography, mathematical logic

5 [File system encryption with integrated user management](#)

Stefan Ludwig, Winfried Kalfa

October 2001 **ACM SIGOPS Operating Systems Review**, Volume 35 Issue 4

Full text available:  [pdf\(655.38 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Existing cryptographic file systems for Unix do not take into account that sensitive data must often be shared with other users, but still kept secret. By design, the only one who has access to the secret data is the person who encrypted it and therefore knows the encryption key or password. This paper presents a kernel driver for a new encrypted file system, called Fairly Secure File System (FSFS), which provides mechanisms for user management and access control for encrypted files. The driver ...

6 [Authentication in the Taos operating system](#)

Edward Wobber, Martín Abadi, Michael Burrows, Butler Lampson

December 1993 **ACM SIGOPS Operating Systems Review , Proceedings of the fourteenth ACM symposium on Operating systems principles**, Volume 27 Issue 5

Full text available:  [pdf\(1.45 MB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We describe a design and implementation of security for a distributed system. In our system, applications access security services through a narrow interface. This interface provides a notion of identity that includes simple principals, groups, roles, and delegations. A new operating system component manages principals, credentials, and secure channels. It checks credentials according to the formal rules of a logic of authentication. Our implementation is efficient enough to support a substantia ...

7 [OCB: A block-cipher mode of operation for efficient authenticated encryption](#)

Phillip Rogaway, Mihir Bellare, John Black

August 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 3

Full text available:  [pdf\(568.74 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We describe a parallelizable block-cipher mode of operation that simultaneously provides privacy and authenticity. OCB encrypts-and-authenticates a nonempty string M and $\lceil n/2 \rceil$ using $\lceil M \rceil/n + 2$ block-cipher invocations, where n is the block length of the underlying block cipher. Additional overhead is small. OCB refines a

scheme, IAPM, suggested by Charanjit Jutla. Desirable properties of OCB include the ability to encrypt a bi ...

Keywords: AES, authenticity, block-cipher usage, cryptography, encryption, integrity, modes of operation, provable security, standards

8 Encryption and Secure Computer Networks

Gerald J. Popek, Charles S. Kline

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4


Full text available:  [pdf\(2.50 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)



9 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles**, Volume 33 Issue 5

Full text available:  [pdf\(1.77 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)



No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use. We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

10 A fast MPEG video encryption algorithm

Changgui Shi, Bharat Bhargava

September 1998 **Proceedings of the sixth ACM international conference on Multimedia**

Full text available:  [pdf\(805.58 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)



Keywords: DES, MPEG codec, MPEG video encryption, multimedia data security

11 Authentication in distributed systems: theory and practice

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber

November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4

Full text available:  [pdf\(3.37 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)




We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegated authority. The theory shows how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We ...

Keywords: certification authority, delegation, group, interprocess communication, key distribution, loading programs, path name, principal, role, secure channel, speaks for, trusted computing base

12 Authentication in distributed systems: theory and practice


Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber

September 1991 **ACM SIGOPS Operating Systems Review , Proceedings of the thirteenth ACM symposium on Operating systems principles**, Volume 25 Issue 5Full text available:  [pdf\(2.33 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegation of authority. The theory explains how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We use the th ...

13 Decentralized storage systems: Farsite: federated, available, and reliable storage for an incompletely trusted environment


Atul Adya, William J. Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, John R. Douceur, Jon Howell, Jacob R. Lorch, Marvin Theimer, Roger P. Wattenhofer

December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SIFull text available:  [pdf\(1.87 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#)

Farsite is a secure, scalable file system that logically functions as a centralized file server but is physically distributed among a set of untrusted computers. Farsite provides file availability and reliability through randomized replicated storage; it ensures the secrecy of file contents with cryptographic techniques; it maintains the integrity of file and directory data with a Byzantine-fault-tolerant protocol; it is designed to be scalable by using a distributed hint mechanism and delegatio ...

14 Papers: Context-agile encryption for high speed communication networks

Lyndon G. Pierson, Edward L. Witzke, Mark O. Bean, Gerry J. Trombley

January 1999 **ACM SIGCOMM Computer Communication Review**, Volume 29 Issue 1Full text available:  [pdf\(1.43 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#)

Different applications have different security requirements for data privacy, data integrity, and authentication. Encryption is one technique that addresses these requirements. Encryption hardware, designed for use in high-speed communications networks, can satisfy a wide variety of security requirements if the hardware implementation is key-agile, key length-agile, mode-agile, and algorithm-agile. Hence, context-agile encryption provides enhanced solutions to the secrecy, interoperability, and ...

15 Access Control Models and Mechanisms: Cryptographic access control in a distributed file system

Anthony Harrington, Christian Jensen

June 2003 **Proceedings of the eighth ACM symposium on Access control models and technologies**Full text available:  [pdf\(249.24 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Traditional access control mechanisms rely on a reference monitor to mediate access to protected resources. Reference monitors are inherently centralized and existing attempts to distribute the functionality of the reference monitor suffer from problems of scalability. Cryptographic access control is a new distributed access control paradigm designed for a global federation of information systems. It defines an implicit access control mechanism, which relies exclusively on cryptography to provide ...

Keywords: access control, cryptography, network file systems

16 MPEG Video Encryption Algorithms

Bharat Bhargava, Changgui Shi, Sheng-Yih Wang

September 2004 **Multimedia Tools and Applications**, Volume 24 Issue 1Full text available:  [Publisher Site](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

Multimedia data security is important for multimedia commerce. Previous cryptography studies have focused on text data. The encryption algorithms developed to secure text data may not be suitable to multimedia applications because of the large data size and real time constraint. For multimedia applications, light weight encryption algorithms are attractive.

We present four fast MPEG video encryption algorithms. These algorithms use a secret key to randomly change the sign bits of Discre ...

Keywords: MPEG codec, MPEG video encryption, multimedia data security

17 Security in embedded systems: Design challenges

Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3Full text available:  [pdf\(3.67 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

18 Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm

Mihir Bellare, Tadayoshi Kohno, Chanathip Namprempre

May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2Full text available:  [pdf\(404.99 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The *secure shell* (SSH) protocol is one of the most popular cryptographic protocols on the Internet. Unfortunately, the current SSH authenticated encryption mechanism is insecure. In this paper, we propose several fixes to the SSH protocol and, using techniques from modern cryptography, we prove that our modified versions of SSH meet strong new chosen-ciphertext privacy and integrity requirements. Furthermore, our proposed fixes will require relatively little modification to the SSH protoc ...

Keywords: Authenticated encryption, secure shell, security proofs, stateful decryption

19 Controlled Operation-Based Fast Methods of Data Protection in Automated Control Systems

V. B. Izotov, A. A. Moldovyan, N. A. Moldovyan


June 2001 **Automation and Remote Control**, Volume 62 Issue 6

Full text available:  [Publisher Site](#)Additional Information: [full citation](#), [abstract](#)

A new controlled operation-based approach was proposed to construct fast algorithms of information processing to tackle efficiently the topical problems of information protection in high-performance automated control systems. Design criteria were discussed, and the algebraic and probabilistic characteristics of the controlled dyadic operations were studied. Consideration was given to the promising methods of encryption for wide application in the information-protection facilities of the aut ...

20 [Integrating security in a large distributed system](#)

M. Satyanarayanan

August 1989 **ACM Transactions on Computer Systems (TOCS)**, Volume 7 Issue 3Full text available:  [pdf\(2.90 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Andrew is a distributed computing environment that is a synthesis of the personal computing and timesharing paradigms. When mature, it is expected to encompass over 5,000 workstations spanning the Carnegie Mellon University campus. This paper examines the security issues that arise in such an environment and describes the mechanisms that have been developed to address them. These mechanisms include the logical and physical separation of servers and clients, support for secure communication ...

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2005 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)